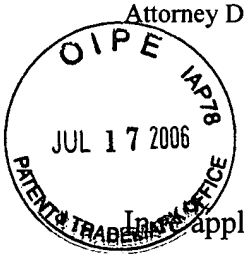
AF
SFW

Attorney Docket No.: 42390P12266 **PATENT**



IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS

In application of:)
)
Minnick)
)
Application No: 09/965,579)
)
Filed: September 26, 2001)
)
For: SECURITY ASSOCIATION MANAGEMENT THROUGH THE USE OF LOOKUP TABLES)

Examiner: Michael J. Pyzocha

Art Unit: 2137

Mail Stop Appeal Brief-Patents
Assistant Commissioner For Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPELLANT'S REPLY TO EXAMINER'S ANSWER
IN SUPPORT OF APPELLANTS' APPEAL AND APPEAL BRIEF
TO THE BOARD OF PATENT APPEALS

Applicant (hereafter "Appellant") hereby submits this Reply in support of the Appeal Brief filed March 3, 2006, and in response to the Examiner's Answer mailed May 12, 2006. Appellant respectfully requests consideration of this Reply by the Board of Patent Appeals for allowance of the invention as presently recited in the claims.

TABLE OF CONTENTS

I. STATUS OF THE CLAIMS/GROUNDS FOR REJECTION 1

II. ARGUMENT 1

III. APPENDIX OF CLAIMS 5

I. STATUS OF THE CLAIMS/GROUNDS FOR REJECTION

Claims 9, 20, 31, and 42 have been canceled.

Claims 1-6, 8, 12-17, 19, 23-28, 30, 34-39, and 41 were rejected under 35 U.S.C. § 102(e) as being unpatentable over a combination of U.S. Patent No. 6,505,192 of Godwin et al. (*Godwin*), U.S. Patent No. 6,763,394 of Tuck, III et al. (*Tuck*), and a webpage based upon an article "Monitoring Ethernet Network Activity with NDIS Drivers" of Apparna et al. (*Apparna*).

Claims 7, 18, 29, and 40 were rejected under 35 U.S.C. § 103(a) as being unpatentable over the primary references in view of Japanese Patent No. 03164866 of Kobayashi et al. (*Kobayashi*).

Claims 10-11, 21-22, 32-33, and 43-44 were rejected under 35 U.S.C. § 103(a) as being unpatentable over the primary references in view of U.S. Patent No. 6,460,122 of Otterness et al. (*Otterness*) and U.S. Patent No. 6,711,562 of Ross et al. (*Ross*).

II. ARGUMENT

Appellant has set forth in previous communications the improperness of the combination of the references, and such arguments will not be repeated herein. However, Appellant maintains the argument that the references are not properly combinable, as well as the other arguments previously made. Nevertheless, Appellant limits the focus of this communication to addressing the merits of the cited references.

Appellant previously set forth the merits of each reference separately, and then discussed the combination of the references. Appellant is thus unable to understand why the Examiner's Answer asserts on page 10 that Appellant has only addressed the references separately. Appellant respectfully submits that the references, whether alone or in combination, fail to disclose or suggest at least one feature of the claimed invention.

As a first matter, Appellant respectfully submits that to provide a prima facie case of obviousness, a reasoned argument must be provided to show with particularity each and every element of the claimed invention in the cited references. Appellant respectfully submits that the Office Actions, as well as the Examiner's Answer fail to address the element of determining if the packet received at the device driver is an ingress packet or an egress packet. Such a feature is cited, for example, in claim 1, which recites:

receiving at a device driver a network packet having a corresponding security association (SA);

determining if the packet is an ingress packet or an egress packet;

determining for the packet a key value corresponding to the SA;

if the packet is an ingress packet, hashing the key value to determine a location of an entry in an **ingress lookup table**, and **if the packet is an egress packet**, hashing the key value to determine a location of an entry in an **egress lookup table**, the entry in the ingress lookup table and the entry in the egress lookup table containing information corresponding to the SA, the ingress lookup table being a separate lookup table from the egress lookup table;

retrieving from the entry an index to a location of the SA in memory; and

retrieving the SA from memory based on the index.

The determination of whether the packet is an ingress or egress packet is performed to determine which of two separate SA lookup tables will apply. It is assumed in Godwin that no such determination applies, because Godwin fails to disclose or suggest separate lookup tables, as mentioned in the Examiner's Answer at page 6. The Examiner's Answer then asserts that Tuck discloses such determining. Appellant traverses.

Tuck discusses determining in a network router whether to pass packets from an ingress port to an egress port, or whether to drop the packets. See Abstract. Tuck makes no determination of whether a packet is an ingress or egress packet. In Tuck, all packets are forwarded through the device. A packet that is received (ingress) is also an outbound packet (egress), unless the packet is dropped. The only determination that is made is whether to drop the packet, not whether the packet is ingress or egress. According to the reference, in one implementation packets are only dropped on ingress (col. 5, lines 8 to 10), but the reference goes on in col. 5, lines 11 to 26 to discuss that a lookup is also performed at egress. Thus, Appellant submits that according to the reference, no determination of whether a packet is an ingress or egress packet is made, and none is needed because according to the system of Tuck, a lookup is performed at both ingress and egress.

Appellant thus submits that the Godwin reference and the Tuck reference, whether alone or in any possible combination, fail to disclose or suggest determining whether a packet received at a device driver is an ingress or egress packet, as recited in the claimed invention. The cited references thus fail to disclose or suggest at least one element of the claimed invention, and so fail to render obvious the invention as recited in the claims.

The looking up of a pass/drop rule at an ingress port and the separate looking up of a pass-drop rule at an egress port of a packet forwarding device (i.e., a router) as discussed in Tuck fails to apply to the lookup of Security Associations within a device driver, as recited in Appellant's claims. The separate looking up of pass/drop rules at an ingress port and an egress port of a router fail to apply to the application of IPSec at network nodes as discussed in Godwin. Each reference is deficient separately, and no combination of the references can be reasonably interpreted as supporting a rejection of the claimed invention, for at least the reasons set forth above.

As discussed previously, and as shown by the arguments in the Examiner's Answer at page 12, Apparna is not cited for, nor does it cure the deficiencies pointed out above. Thus, combining the references discussed above with Apparna fails to render obvious the claimed invention.

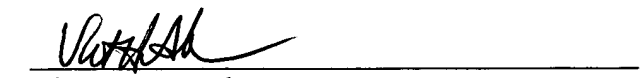
VIII. CONCLUSION

Appellant respectfully submits this Reply as a matter of right, filed within the two month deadline of the mailing date of the Examiner's Answer. Appellant respectfully submits that all appealed claims in this application are patentable and request that the Board of Patent Appeals overrule the Examiner and direct allowance of the rejected claims.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP

Date: July 12, 2006



Vincent H. Anderson
Reg. No. 54,962

12400 Wilshire Blvd., 7th Floor
Los Angeles, CA 90025-1026
Telephone: (503) 439-8778

I hereby certify that this correspondence is being deposited with the United States Postal service as first class mail on the below date with sufficient postage in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450

Signature  7/12/06
Gayle Bekish Date

APPENDIX A: CLAIMS ON APPEAL

1. (Previously Presented) A method comprising:

receiving at a device driver a network packet having a corresponding security association (SA);

determining if the packet is an ingress packet or an egress packet;

determining for the packet a key value corresponding to the SA;

if the packet is an ingress packet, hashing the key value to determine a location of an entry in an ingress lookup table, and if the packet is an egress packet, hashing the key value to determine a location of an entry in an egress lookup table, the entry in the ingress lookup table and the entry in the egress lookup table containing information corresponding to the SA, the ingress lookup table being a separate lookup table from the egress lookup table;

retrieving from the entry an index to a location of the SA in memory; and

retrieving the SA from memory based on the index.

2. (Previously Presented) The method of claim 1 wherein receiving the network packet comprises the device driver being passed an egress packet from an electronic system operating system.

3. (Previously Presented) The method of claim 1 wherein receiving the network packet comprises the device driver being passed an ingress packet from a network interface device.

4. (Original) The method of claim 1 wherein the key value is a handle created for the SA for an egress packet.

5. (Original) The method of claim 1 wherein the key value is a security parameter index (SPI) extracted from the packet for an ingress packet.

6. (Original) The method of claim 1 wherein the lookup table entry comprises the key value and the index.

7. (Original) The method of claim 6 wherein the lookup table entry further comprises a counter to track collisions for the entry.

8. (Previously Presented) The method of claim 1 further comprising the location in memory of an SA corresponding to egress traffic being in a first table, and the location in memory of an SA corresponding to ingress traffic being in a second table, the tables being separate tables in memory.

9. (Canceled)

10. (Original) The method of claim 1 further comprising supporting a number of network traffic streams, wherein the lookup table has 2^N entries, where N is an integer, 2^N being the lowest binary number greater than five times the number of network traffic streams supported.

11. (Previously Presented) The method of claim 1 wherein hashing the key value comprises using a bit-wise AND hash function with a mask of value 2^N-1, where N is an integer, wherein the hash table contains 2^N entries.

12. (Previously Presented) An article comprising a machine-accessible medium to provide content to cause one or more electronic systems to:

receive at a device driver a network packet having a corresponding security association (SA);

determine if the packet is an ingress packet or an egress packet;

determine for the packet a key value corresponding to the SA;

if the packet is an ingress packet, hash the key value to determine a location of an entry in an ingress lookup table, and if the packet is an egress packet, hash the key value to determine a location of an entry in an egress lookup table, the entry in the ingress lookup table and the entry in the egress lookup table containing information corresponding to the SA, the ingress lookup table being a separate lookup table from the egress lookup table;

retrieve from the entry an index to a location of the SA in memory; and

retrieve the SA from memory based on the index.

13. (Previously Presented) The article of claim 12 wherein to receive the network packet comprises the device driver to be passed an egress packet from an electronic system operating system.

14. (Previously Presented) The article of claim 12 wherein to receive the network packet comprises the device driver to be passed an ingress packet from a network interface device.

15. (Original) The article of claim 12 wherein the key value is a handle created for the SA for an egress packet.

16. (Original) The article of claim 12 wherein the key value is a security parameter index (SPI) extracted from the packet for an ingress packet.

17. (Original) The article of claim 12 wherein the lookup table entry comprises the key value and the index.

18. (Original) The article of claim 17 wherein the lookup table entry further comprises a counter to track collisions for the entry.

19. (Previously Presented) The article of claim 12 further comprising the location in memory of an SA corresponding to egress traffic being in a first table, and the location in memory of an SA corresponding to ingress traffic being in a second table, the tables being separate tables in memory.

20. (Canceled)

21. (Original) The article of claim 12 further comprising to support a number of network traffic streams, wherein the lookup table has 2^N entries, where N is an integer, 2^N being the lowest binary number greater than five times the number of network traffic streams supported.

22. (Previously Presented) The article of claim 12 wherein to hash the key value comprises using a bit-wise AND hash function with a mask of value 2^N-1, where N is an integer, wherein the hash table contains 2^N entries.

23. (Withdrawn) An electronic data signal embodied in a data communications medium shared among a plurality of network devices comprising content to cause one or more electronic systems to:

receive at a device driver a network packet having a corresponding security association (SA);

determine if the packet is an ingress packet or an egress packet;

determine for the packet a key value corresponding to the SA;

if the packet is an ingress packet, hash the key value to determine a location of an entry in an ingress lookup table, and if the packet is an egress packet, hash the key value to determine a location of an entry in an egress lookup table, the entry in the ingress lookup table and the entry in the egress lookup table containing information corresponding to the SA, the ingress lookup table being a separate lookup table from the egress lookup table;

retrieve from the entry an index to a location of the SA in memory; and

retrieve the SA from memory based on the index.

24. (Withdrawn) The electronic data signal of claim 23 wherein to receive the network packet comprises the device driver to be passed an egress packet from an electronic system operating system.

25. (Withdrawn) The electronic data signal of claim 23 wherein to receive the network packet comprises the device driver to be passed an ingress packet from a network interface device.

26. (Original) The electronic data signal of claim 23 wherein the key value is a handle created for the SA for an egress packet.

27. (Original) The electronic data signal of claim 23 wherein the key value is a security parameter index (SPI) extracted from the packet for an ingress packet.

28. (Original) The electronic data signal of claim 23 wherein the lookup table entry comprises the key value and the index.

29. (Original) The electronic data signal of claim 28 wherein the lookup table entry further comprises a counter to track collisions for the entry.

30. (Withdrawn) The electronic data signal of claim 23 further comprising the location in memory of an SA corresponding to egress traffic being in a first table, and the location in memory of an SA corresponding to ingress traffic being in a second table, the tables being separate tables in memory.

31. (Canceled)

32. (Withdrawn) The electronic data signal of claim 23 further comprising to support a number of network traffic streams, wherein the lookup table has 2^N entries, where N is an integer, 2^N being the lowest binary number greater than five times the number of network traffic streams supported.

33. (Withdrawn) The electronic data signal of claim 23 wherein to hash the key value comprises using a bit-wise AND hash function with a mask of value 2^N-1, where N is an integer, wherein the hash table contains 2^N entries.

34. (Previously Presented) An electronic system comprising:

one or more processors;

a network interface coupled with the one or more processors to provide a communications path between the electronic system and a network, the network interface to have a corresponding device driver to be executed on one or more of the processors; and

a memory coupled with the one or more processors, the memory to have a program to provide instructions for the electronic system to receive at the device driver a network packet having a corresponding security association (SA), the program to determine if the packet is an

ingress packet or an egress packet, to determine for the packet a key value corresponding to the SA, and if the packet is an ingress packet, hash the key value to determine a location of an entry in an ingress lookup table, and if the packet is an egress packet, hash the key value to determine a location of an entry in an egress lookup table, the entry in the ingress lookup table and the entry in the egress lookup table containing information corresponding to the SA, the ingress lookup table being a separate lookup table from the egress lookup table, to retrieve from the entry an index to a location of the SA in memory, and to retrieve the SA from memory based on the index.

35. (Previously Presented) The electronic system of claim 34 wherein the program to receive the network packet comprises the device driver to be passed an egress packet from an operating system.

36. (Previously Presented) The electronic system of claim 34 wherein the program to receive the network packet comprises the device driver to be passed an ingress packet from the network interface.

37. (Original) The electronic system of claim 34 wherein the key value is a handle created for the SA for an egress packet.

38. (Original) The electronic system of claim 34 wherein the key value is a security parameter index (SPI) extracted from the packet for an ingress packet.

39. (Original) The electronic system of claim 34 wherein the lookup table entry comprises the key value and the index.

40. (Original) The electronic system of claim 39 wherein the lookup table entry further comprises a counter to track collisions for the entry.

41. (Previously Presented) The electronic system of claim 34 further comprising the location in memory of an SA corresponding to egress traffic being in a first table, and the location in memory of an SA corresponding to ingress traffic being in a second table, the tables being separate tables in memory.

42. (Canceled)

43. (Original) The electronic system of claim 34 further comprising the program to support a number of network traffic streams, wherein the lookup table has 2^N entries, where N is an integer, 2^N being the lowest binary number greater than five times the number of network traffic streams supported.

44. (Previously Presented) The electronic system of claim 34 wherein to hash the key value comprises using a bit-wise AND hash function with a mask of value 2^N-1, where N is an integer, wherein the hash table contains 2^N entries.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application No.	09/965, 579
Filing Date	September 26, 2001
First Named Inventor	Linden Minnick
Art Unit	2137
Examiner Name	Michael J. Pyzocha
Total Number of Pages in This Submission	14
Attorney Docket Number	42390P12266

ENCLOSURES ***(check all that apply)***

- ☒ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment / Response
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
  - ☐ PTO/SB/08
- ☐ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
  - ☐ Basic Filing Fee
  - ☐ Declaration/POA
  - ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Drawing(s)
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s)
  - ☐ Landscape Table on CD
- ☐ After Allowance Communication to TC
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☒ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
- ☐ Proprietary Information
- ☐ Status Letter
- ☒ Other Enclosure(s) *(please identify below):*

Return Postcard

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm or Individual name	Jared S. Engstrom, Reg. No. 58,330 BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP
Signature	
Date	July 12, 2006

CERTIFICATE OF MAILING/TRANSMISSION

I hereby certify that this correspondence is being deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop Appeal Brief-Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

Typed or printed name	**Gayle Bekish**		
Signature		Date	**July 12, 2006**

Based on PTO/SB/21 (09-04) as modified by Blakely, Sokoloff, Taylor & Zafman (wlr) 11/30/2005.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

FEE TRANSMITTAL for FY 2005

Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27.

TOTAL AMOUNT OF PAYMENT ($)

Complete if Known	
Application Number	09/965, 579
Filing Date	September 26, 2001
First Named Inventor	Linden Minnick
Examiner Name	Michael J. Pyzocha
Art Unit	2137
Attorney Docket No.	42390P12266

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☐ Credit card ☐ Money Order ☒ None ☐ Other (please identify): _____

☒ Deposit Account Deposit Account Number: 02-2666 Deposit Account Name: Blakely, Sokoloff, Taylor & Zafman LLP

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☐ Charge fee(s) indicated below
☐ Charge fee(s) indicated below, except for the filing fee
☒ Charge any additional fee(s) or underpayment of fee(s) under 37 CFR §§ 1.16, 1.17, 1.18 and 1.20.
☐ Credit any overpayments

FEE CALCULATION

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet.	
2053	130	2053	130	Non-English specification	
1251	120	2251	60	Extension for reply within first month	
1252	450	2252	225	Extension for reply within second month	
1253	1,020	2253	510	Extension for reply within third month	
1254	1,590	2254	795	Extension for reply within fourth month	
1255	2,160	2255	1,080	Extension for reply within fifth month	
1401	500	2401	250	Notice of Appeal	
1402	500	2402	250	Filing a brief in support of an appeal	
1403	1,000	2403	500	Request for oral hearing	
1451	1,510	2451	1,510	Petition to institute a public use proceeding	
1460	130	2460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
1809	790	1809	395	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	790	2810	395	For each additional invention to be examined (37 CFR § 1.129(b))	

Other fee (specify) _____

SUBTOTAL (2) ($)

SUBMITTED BY *Complete (if applicable)*

Name (Print/Type)	Jared S. Engstrom	Registration No. (Attorney/Agent)	58,330	Telephone	(503) 439-8778
Signature				Date	07/12/06

Based on PTO/SB/17 (12-04) as modified by Blakely, Sokoloff, Taylor & Zafman (wlr) 12/15/2004.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450